

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2003-224556
(P2003-224556A)

(43) 公開日 平成15年8月8日 (2003.8.8)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 L 9/08		G 0 9 C 1/00	6 4 0 E 5 J 1 0 4
G 0 9 C 1/00	6 4 0	H 0 4 L 12/28	2 0 0 Z 5 K 0 3 3
H 0 4 L 12/28	2 0 0	9/00	6 0 1 C
			6 0 1 E

審査請求 有 請求項の数28 O L (全 18 頁)

(21) 出願番号 特願2002-19135(P2002-19135)
(22) 出願日 平成14年1月28日 (2002.1.28)

(71) 出願人 000003078
株式会社東芝
東京都港区芝浦一丁目1番1号
(72) 発明者 斉藤 健
神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内
(72) 発明者 中北 英明
神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内
(74) 代理人 100058479
弁理士 鈴江 武彦 (外6名)

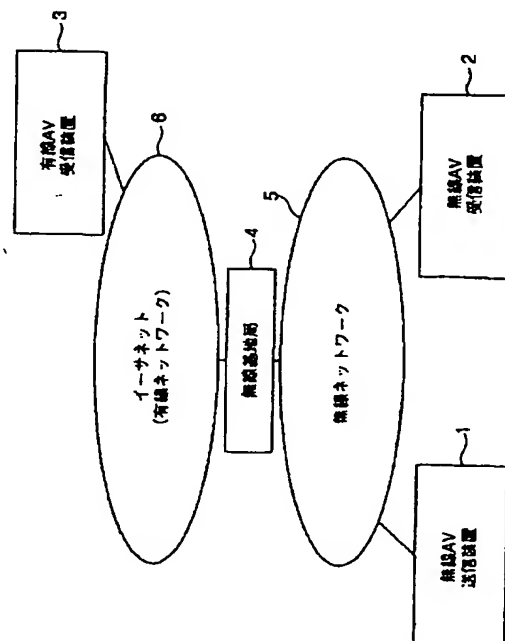
最終頁に続く

(54) 【発明の名称】 通信装置及び通信制御方法

(57) 【要約】

【課題】 著作権を保護すべきAVデータを暗号化して転送し復号して利用できる範囲を、一定の範囲内に制限することの可能な通信装置を提供すること。

【解決手段】 無線AV送信装置1から無線AV受信装置2へ、著作権を保護すべきAVデータを暗号化して、インターネットプロトコル上にて転送する。その際、著作権を保護すべきAVデータの暗号化や復号に使用する暗号鍵は、無線AV送信装置1と無線AV受信装置2との間で認証・鍵交換手順を行うことによって、共有される。この認証・鍵交換手順は、物理ネットワークフレーム上又はデータリンクレイヤネットワークフレーム上にて直接行なわれる。したがって、著作権を保護すべきAVデータをやりとりできる範囲を、IPサブネット内の無線ネットワーク内、あるいはIPサブネット内に限定することができる。



【特許請求の範囲】

【請求項1】著作権を保護すべきコンテンツ・データに暗号化を施して転送する機能を有する通信装置であって、
転送対象となる前記コンテンツ・データに対して著作権保護として暗号化を施す暗号処理手段と、
前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、
前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、
特定の物理ネットワークとのインタフェースとなる物理ネットワークインタフェース手段とを備え、
前記受信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上にて直接行なうことを特徴とする通信装置。

【請求項2】著作権を保護すべきコンテンツ・データに暗号化を施して転送する機能を有する通信装置であって、
転送対象となる前記コンテンツ・データに対して著作権保護として暗号化を施す暗号処理手段と、
前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、
前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、
特定のデータリンクレイヤネットワークとのインタフェースとなるデータリンクレイヤネットワークインタフェース手段とを備え、
前記受信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする通信装置。

【請求項3】著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置であって、
前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、
受信された前記暗号化を施されたコンテンツ・データに対して復号を施す暗号処理手段と、
前記コンテンツ・データの送信側となる通信装置との間で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、

特定の物理ネットワークとのインタフェースとなる物理ネットワークインタフェース手段とを備え、
前記送信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上にて直接行なうことを特徴とする通信装置。

【請求項4】著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置であって、
前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、
受信された前記暗号化を施されたコンテンツ・データに対して著作権保護としての復号を施す暗号処理手段と、
前記コンテンツ・データの送信側となる通信装置との間で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、
特定のデータリンクレイヤネットワークとのインタフェースとなるデータリンクレイヤネットワークインタフェース手段とを備え、
前記送信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする通信装置。

【請求項5】前記物理ネットワークフレームは、無線フレームであることを特徴とする請求項1または3に記載の通信装置。

【請求項6】前記データリンクレイヤネットワークフレームは、イーサネット（登録商標）フレームであることを特徴とする請求項2または4に記載の通信装置。

【請求項7】前記認証・鍵交換処理手段により行われる前記認証・鍵交換の手続きの対象とするコンテンツ・データを特定するための所定の情報を、当該認証・鍵交換の手続きのためにやりとりされるデータ内に記述することを特徴とする請求項1ないし6のいずれか1項に記載の通信装置。

【請求項8】前記コンテンツ・データは、AVデータ、前記ネットワークレイヤプロトコルは、インターネットプロトコルである場合に、前記所定の情報として、AVストリームの送信側装置のIPアドレスとポート番号及び受信側装置のIPアドレスとポート番号の全部又は一部を用いることを特徴とする請求項7に記載の通信装置。

【請求項9】前記コンテンツ・データは、AVデータ、前記ネットワークレイヤプロトコルは、インターネットプロトコルである場合に、前記所定の情報として、AVストリームのRTPパケットに含まれるSSRCの値を用いることを特徴とする請求項7に記載の通信装置。

【請求項10】前記コンテンツ・データは、AVデー

タ、前記ネットワークレイヤプロトコルは、インターネットプロトコルである場合に、前記所定の情報として、AVストリームが転送されるIPパケットに含まれるフローIDの値を用いることを特徴とする請求項7に記載の通信装置。

【請求項11】前記認証・鍵交換処理手段により行われる前記認証・鍵交換の手続きは、特定のコンテンツ・データが著作権保護としての暗号化を施された上で転送されることについて送信側となる通信装置から受信側となる通信装置へ通知する手続きを含むことを特徴とする請求項7に記載の通信装置。

【請求項12】前記認証・鍵交換処理手段により行われる前記認証・鍵交換の手続きは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含み、

前記コンテンツ・データは、前記著作権保護用制御データを含まずに転送されるものであることを特徴とする請求項7に記載の通信装置。

【請求項13】著作権を保護すべきコンテンツ・データであって著作権保護用制御データを含まないものに暗号化を施して転送する機能を有する通信装置であって、転送対象となる前記コンテンツ・データに対して著作権保護としての暗号化を施す暗号処理手段と、前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上に行うための転送処理手段と、前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段とを備え、前記認証・鍵交換処理手段により行われる前記認証・鍵交換の手続きは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする通信装置。

【請求項14】著作権保護としての暗号化を施されたコンテンツ・データであって著作権保護用制御データを含まないものを受信し復号する機能を有する通信装置であって、前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上に行うための転送処理手段と、受信された前記暗号化を施されたコンテンツ・データに対して復号を施す暗号処理手段と、前記コンテンツ・データの送信側となる通信装置との間で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段とを備え、前記認証・鍵交換処理手段により行われる前記認証・鍵

交換の手続きは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする通信装置。

【請求項15】前記著作権保護用制御データは、暗号管理情報又は暗号再計算タイミングの少なくとも一方を含むものであることを特徴とする請求項12ないし14のいずれか1項に記載の通信装置。

【請求項16】前記コンテンツ・データの処理を行なうコンテンツ・データ処理手段を更に備えたことを特徴とする請求項1ないし15のいずれか1項に記載の通信装置。

【請求項17】前記ネットワークレイヤプロトコルは、インターネットプロトコルであることを特徴とする請求項1ないし16のいずれか1項に記載の通信装置。

【請求項18】前記コンテンツ・データは、AVデータであることを特徴とする請求項1ないし17のいずれか1項に記載の通信装置。

【請求項19】著作権を保護すべきコンテンツ・データに暗号化を施してネットワークレイヤプロトコル上にて転送する機能を有する通信装置における通信制御方法であって、

前記著作権保護としての暗号化を施されたコンテンツ・データの受信側となる通信装置から、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なうことの要求を直接搭載した物理ネットワークフレーム又はデータリンクレイヤネットワークフレームを受信し、前記受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上又は前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする通信制御方法。

【請求項20】著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置における通信制御方法であって、前記著作権保護としての暗号化を施されたコンテンツ・データの送信側となる通信装置へ、前記著作権保護としての暗号化及び前記復号のための認証・鍵交換の手続きを行なうことの要求を直接搭載した物理ネットワークフレーム又はデータリンクレイヤネットワークフレームを送信し、前記送信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上又は前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする通信制御方法。

【請求項21】著作権を保護すべきコンテンツ・データ

であって著作権保護用制御データを含まないものに暗号化を施してネットワークレイヤプロトコル上にて転送する機能を有する通信装置における通信制御方法であって、

前記著作権保護としての暗号化を施されたコンテンツ・データの受信側となる通信装置から、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なうことの要求を受信する第1のステップと、

前記受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きのためのデータのやりとりを行なう第2のステップとを有し、

前記第2のステップは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする通信制御方法。

【請求項22】著作権保護としての暗号化を施されたコンテンツ・データであって著作権保護用制御データを含まないものを受信し復号する機能を有する通信装置における通信制御方法であって、

前記著作権保護としての暗号化を施されたコンテンツ・データの送信側となる通信装置へ、前記著作権保護としての暗号化及び前記復号のための認証・鍵交換の手続きを行なうことの要求を送信する第1のステップと、

前記送信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きのためのデータのやりとりを行なう第2のステップとを有し、

前記第2のステップは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする通信制御方法。

【請求項23】著作権を保護すべきコンテンツ・データに暗号化を施して転送する機能を有する通信装置としてコンピュータを機能させるためのプログラムであって、転送対象となる前記コンテンツ・データに対して著作権保護として暗号化を施す暗号処理機能と、

前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理機能と、

前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理機能と、

特定の物理ネットワークとのインタフェースとなる物理ネットワークインタフェース機能としてコンピュータを実現させ、

前記受信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネット

ワークフレーム上にて直接行なわせるためのプログラム。

【請求項24】著作権を保護すべきコンテンツ・データに暗号化を施して転送する機能を有する通信装置としてコンピュータを機能させるためのプログラムであって、転送対象となる前記コンテンツ・データに対して著作権保護として暗号化を施す暗号処理機能と、

前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理機能と、

前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理機能と、

特定のデータリンクレイヤネットワークとのインタフェースとなるデータリンクレイヤネットワークインタフェース機能としてコンピュータを実現させ、

前記受信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記データリンクレイヤネットワークフレーム上にて直接行なわせるためのプログラム。

【請求項25】著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置としてコンピュータを機能させるためのプログラムであって、

前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理機能と、

受信された前記暗号化を施されたコンテンツ・データに対して復号を施す暗号処理機能と、

前記コンテンツ・データの送信側となる通信装置との間で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理機能と、

特定の物理ネットワークとのインタフェースとなる物理ネットワークインタフェース機能としてコンピュータを実現させ、

前記送信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上にて直接行なわせるためのプログラム。

【請求項26】著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置であって、

前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理機能と、

受信された前記暗号化を施されたコンテンツ・データに対して著作権保護としての復号を施す暗号処理機能と、

前記コンテンツ・データの送信側となる通信装置との間

で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理機能と、

特定のデータリンクレイヤネットワークとのインタフェースとなるデータリンクレイヤネットワークインタフェース機能としてコンピュータを実現させ、

前記送信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記データリンクレイヤネットワークフレーム上にて直接行なわせるためのプログラム。

【請求項27】著作権を保護すべきコンテンツ・データであって著作権保護用制御データを含まないものに暗号化を施して転送する機能を有する通信装置としてコンピュータを機能させるためのプログラムであって、転送対象となる前記コンテンツ・データに対して著作権保護として暗号化を施す暗号処理機能と、前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理機能と、

前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きであって、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むものを行なう認証・鍵交換処理機能とをコンピュータに実現させるためのプログラム。

【請求項28】著作権保護としての暗号化を施されたコンテンツ・データであって著作権保護用制御データを含まないものを受信し復号する機能を有する通信装置としてコンピュータを機能させるためのプログラムであって、

前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理機能と、

受信された前記暗号化を施されたコンテンツ・データに対して復号を施す暗号処理機能と、

前記コンテンツ・データの送信側となる通信装置との間で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きであって、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むものを行なう認証・鍵交換処理機能とをコンピュータに実現させるためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、著作権保護機能を持ってAVデータのやり取りを行なう通信装置及び通信制御方法に関する。

【0002】

【従来の技術】デジタル情報家電と呼ばれる商品が増加している。これらは、デジタル放送の開始などに伴い、普及が期待される商品群であり、デジタル放送対応テレビや、セットトップボックス、デジタルVTR、DVDプレーヤ、ハードディスクレコーダ等、デジタルデータ・デジタルコンテンツを扱う商品が広く含まれる。

【0003】この際、考慮すべきは著作権保護である。デジタルデータは、コピー時の品質劣化が無いなどの利点が強調される反面、不正コピーが容易であるなどの欠点も持つ。

【0004】このため、デジタルAV機器同士をつなぐデジタルネットワークであるIEEE1394には、認証・鍵交換機構や、データの暗号化の機能を兼ね備えられている。

【0005】

【発明が解決しようとする課題】ここで、ある送信装置から、著作権を保護すべきAVデータ（ただし、暗号化したもの）を、受信装置に転送する場合を考える。当該AVデータをやりとりする範囲（ただし、受信装置が復号できる範囲）は、一定の範囲内（例えば、当該AVデータを使用できる正当な権限の範囲内（例えば、著作権30条の私的使用の範囲内）あるいはそれよりもさらに狭い範囲内）に制限され、そのような範囲を越えてのAVデータのやりとりは（視聴料や著作権料等の支払いが伴うようにするなどの措置を考えない限りは）できないようにされるのが望ましい。

【0006】一定の範囲内でのAVデータのやり取りの典型的な例は、IEEE1394や無線ネットワーク等のホームネットワークに閉じた通信である。

【0007】一定の範囲内を越えたAVデータのやり取りの典型的な例は、「公衆網（例えば、インターネットや、電話網等）」を介したやり取りである。

【0008】近い将来、デジタルネットワークの種類は、無線、パソコンネットワーク等と、色々な種類に増加するものと考えられるが、これらの多くでは著作権保護は考慮されていないのが現状である。

【0009】また、ネットワークはローカルなものから、グローバルなものまで幅広くあり、著作権保護の観点からは明確に区別されるのが望ましい。

【0010】本発明は、上記事情を考慮してなされたもので、著作権を保護すべきコンテンツ・データを暗号化して転送し復号して利用できる範囲を、一定の範囲内に制限することの可能な通信装置及び通信制御方法を提供することを目的とする。

【0011】

【課題を解決するための手段】本発明は、著作権を保護すべきコンテンツ・データに暗号化を施して転送する機能を有する通信装置であって、転送対象となる前記コンテンツ・データに対して著作権保護として暗号化を施す暗号処理手段と、前記著作権保護としての暗号化を施さ

れたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、特定の物理ネットワークとのインタフェースとなる物理ネットワークインタフェース手段とを備え、前記受信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上にて直接行なうことを特徴とする。

【0012】本発明は、著作権を保護すべきコンテンツ・データに暗号化を施して転送する機能を有する通信装置であって、転送対象となる前記コンテンツ・データに対して著作権保護としての暗号化を施す暗号処理手段と、前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、特定のデータリンクレイヤネットワークとのインタフェースとなるデータリンクレイヤネットワークインタフェース手段とを備え、前記受信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする。

【0013】本発明は、著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置であって、前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、受信された前記暗号化を施されたコンテンツ・データに対して復号を施す暗号処理手段と、前記コンテンツ・データの送信側となる通信装置との間で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、特定の物理ネットワークとのインタフェースとなる物理ネットワークインタフェース手段とを備え、前記送信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上にて直接行なうことを特徴とする。

【0014】本発明は、著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置であって、前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、受信された前記暗号化を施されたコンテンツ・データに対して著作権保護としての復号を施す暗号処理手段と、前記コンテンツ・データの送信側となる通信装置との間

で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、特定のデータリンクレイヤネットワークとのインタフェースとなるデータリンクレイヤネットワークインタフェース手段とを備え、前記送信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする。

【0015】本発明は、著作権を保護すべきコンテンツ・データであって著作権保護用制御データを含まないものに暗号化を施して転送する機能を有する通信装置であって、転送対象となる前記コンテンツ・データに対して著作権保護としての暗号化を施す暗号処理手段と、前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段とを備え、前記認証・鍵交換処理手段により行われる前記認証・鍵交換の手続きは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする。

【0016】本発明は、著作権保護としての暗号化を施されたコンテンツ・データであって著作権保護用制御データを含まないものを受信し復号する機能を有する通信装置であって、前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、受信された前記暗号化を施されたコンテンツ・データに対して復号を施す暗号処理手段と、前記コンテンツ・データの送信側となる通信装置との間で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段とを備え、前記認証・鍵交換処理手段により行われる前記認証・鍵交換の手続きは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする。

【0017】本発明は、著作権を保護すべきコンテンツ・データに暗号化を施してネットワークレイヤプロトコル上にて転送する機能を有する通信装置における通信制御方法であって、前記著作権保護としての暗号化を施されたコンテンツ・データの受信側となる通信装置から、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なうことの要求を直接搭載した物理ネットワークフレーム又はデータリンクレイヤネットワークフレームを受信し、前記受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のため

の認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上又は前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする。

【0018】本発明は、著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置における通信制御方法であって、前記著作権保護としての暗号化を施されたコンテンツ・データの送信側となる通信装置へ、前記著作権保護としての暗号化及び前記復号のための認証・鍵交換の手続きを行なうことの要求を直接搭載した物理ネットワークフレーム又はデータリンクレイヤネットワークフレームを送信し、前記送信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上又は前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする。

【0019】本発明は、著作権を保護すべきコンテンツ・データであって著作権保護用制御データを含まないものに暗号化を施してネットワークレイヤプロトコル上にて転送する機能を有する通信装置における通信制御方法であって、前記著作権保護としての暗号化を施されたコンテンツ・データの受信側となる通信装置から、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なうことの要求を受信する第1のステップと、前記受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きのためのデータのやりとりを行なう第2のステップとを有し、前記第2のステップは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする。

【0020】本発明は、著作権保護としての暗号化を施されたコンテンツ・データであって著作権保護用制御データを含まないものを受信し復号する機能を有する通信装置における通信制御方法であって、前記著作権保護としての暗号化を施されたコンテンツ・データの送信側となる通信装置へ、前記著作権保護としての暗号化及び前記復号のための認証・鍵交換の手続きを行なうことの要求を送信する第1のステップと、前記送信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きのためのデータのやりとりを行なう第2のステップとを有し、前記第2のステップは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする。

【0021】なお、装置に係る本発明は方法に係る発明

としても成立し、方法に係る本発明は装置に係る発明としても成立する。また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムとしても成立し、該プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0022】本発明によれば、著作権を保護すべきコンテンツ・データを暗号化して転送し復号して利用できる範囲を、一定の範囲内（例えば、同一のIPサブネット内における1つの無線ネットワーク内、同一のIPサブネット内）に制限することができる。

【0023】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【0024】図1に、本実施形態のネットワークシステムの構成例を示す。

【0025】図1は、ある家庭の家庭ネットワークと、これに接続されたネットワーク機器を示している。もちろん、図1に示したネットワーク機器以外に、他のネットワーク機器や、その他の装置が存在しても構わない。

【0026】図1に例示されるように、この家庭には、家庭ネットワークとして、イーサネット（有線ネットワーク）6と無線ネットワーク5が存在し、これらが無線基地局（無線アクセスポイント）4で相互接続されている。この無線基地局4は、ブリッジ（イーサネットブリッジ）の役割を果たす。無線ネットワーク5上でも、イーサネットフレーム（あるいは、これに順ずる形）で、パケットは転送されるものとする（ただし、これに限定するものではない）。例えば、IEEE802.11aや、IEEE802.11b等の無線LANがこれにあたる。さらに、無線ネットワーク5には、無線AV送信装置1と、無線AV受信装置2が、イーサネット6には有線AV受信装置3が、それぞれ接続されている。

【0027】無線AV送信装置1と、無線AV受信装置2との間では、AVデータのやり取りを行なう。無線AV送信装置1と、有線AV受信装置3との間についても同様である。無線AV送信装置1は、セットトップボックスやDVDプレーヤ等といったAVデータのソースデバイスとなり得る機器であり、無線AV受信装置2や有線AV受信装置3は、テレビやディスプレイ、スピーカ、あるいは録画・録音装置といった、AVデータのシンクデバイスとなり得る機器である。

【0028】図2に、無線AV送信装置1の内部構成例を示す。

【0029】図2に示されるように、無線AV送信装置1は、AVデータの生成や蓄積を行い、ネットワークに送出するAVデータのソースとなるAVデータ生成／蓄積部11、タイムスタンプ処理やシーケンス番号処理

等、これらのAVデータのトランスポートレイヤ層の処理を行なうRTP処理部12、これらのパケットをTCP/IPのパケットで送受信するTCP/IPパケット送受信部13、暗号化等の著作権保護の処理が必要なデータに関して、AVデータの暗号化処理を行なう著作権保護暗号化部14、イーサネットフレームを送受信するイーサネットフレーム送受信部15、IPアドレスとイーサネットアドレスの対応を取るためのIP/イーサネットアドレス対応テーブル16、著作権保護のために、AV受信装置との間で認証や鍵交換等を行なうための著作権保護認証・鍵交換部17、無線ネットワークとのインタフェース部（無線ネットワークI/F部）18を備えている。

【0030】図3に、無線AV受信装置2の内部構成例を示す。

【0031】図3に示されるように、無線AV受信装置2は、無線ネットワークとのインタフェース部（無線ネットワークI/F部）28、イーサネットフレームを送受信するイーサネットフレーム送受信部25、著作権保護のために暗号化されて転送されてきたAVデータを復号化する著作権保護復号化部24、これらのパケットをTCP/IPのパケットで送受信するTCP/IPパケット送受信部23、タイムスタンプ処理やシーケンス番号処理等、これらのAVデータのトランスポートレイヤ層の処理を行なうRTP処理部22、受信したAVデータの再生や蓄積（録音や録画）を行い、AVデータのシンクとなるAVデータ再生/蓄積部21、IPアドレスとイーサネットアドレスの対応を取るためのIP/イーサネットアドレス対応テーブル26、著作権保護のために、AV送信装置との間で認証や鍵交換等を行なうための著作権保護認証・鍵交換部27を備えている。

【0032】また、図4に、有線AV受信装置3の内部構成例を示す。

【0033】図4に示されるように、イーサネットに接続される有線AV受信装置3は、基本的には、図3の無線AV受信装置2と同様の構成を有する（なお、イーサネットに接続されることから、図3の無線ネットワークインタフェース部の代わりに、イーサネットインタフェース部（イーサネットI/F部）38を有する）。ただし、後述するように、無線AV受信装置2が無線AV送信装置1との間で行なう著作権保護のための認証や鍵交換の少なくとも一部は、無線制御フレーム上にてやり取りがなされる。このため、有線AV受信装置3は無線制御フレームをやり取りする機能を持たないことから、著作権保護認証・鍵交換部37でやり取りされる著作権保護用の制御データは、無線AV受信装置2のそれと異なり、イーサネットフレームなり、IPパケットなりの形で転送される点も、無線AV受信装置と相違する点である。

【0034】次に、本実施形態の家庭ネットワークシス

テムにおいてやり取りされるパケットのフォーマットについて説明する。

【0035】TCP/IPパケットは、無線ネットワーク5、イーサネット6の両方のネットワークにおいて、どちらもイーサネットフレームにカプセル化されて転送される。ネットワークがイーサネットの場合は、このイーサネットフレーム（イーサネットヘッダ+TCP/IPパケット）の形でパケットが転送される。一方、ネットワークが無線ネットワークの場合には、上記のイーサネットフレームに、さらに無線レイヤヘッダが付与される形で、（無線レイヤヘッダ+イーサネットヘッダ+TCP/IPパケット）の形で転送される。なお、トレイラについてはプロトコルに準ずればよい（トレイラを使用するプロトコルであってもよいし、そうでないプロトコルであってもよい）。

【0036】図5に、無線レイヤフレームのフォーマットの一例を示す。

【0037】無線レイヤヘッダには、無線ネットワーク5上でのみ使用する制御データ（例えば、802.11無線LANにおけるFCフィールドや、Dur/IDフィールド等）等が含まれる。このFCフィールドには、2ビットのTypeフィールドが含まれており、無線レイヤフレームの種類が示される。Typeフィールドが0ならば管理用、1ならば制御用、2ならば通常データ用である。管理用無線レイヤフレームとして代表的なものは、ビーコンであり、周期的にネットワークに配信されて、各無線AV装置の無線レイヤにおけるクロックを調整するために、主に使用される。そのほか、プローブ要求および応答、認証関係構築および解消、ネットワークへの参加要求および応答などがある。一方、制御用無線レイヤフレームには、送信期間設定に関するもの、受信確認に関するものなどがある。

【0038】上記著作権保護用の制御データは、管理用無線レイヤフレーム、制御用無線レイヤフレーム、または、Typeフィールドが3であるような新たな種類の無線レイヤフレームのいずれかによって扱うことができ、後述の著作権保護シーケンスに適用可能である。

【0039】どの種類のフレームでも、FCフィールドに、4ビットのSubTypeフィールドがさらに含まれており、現在はリザーブされているSubTypeを、著作権保護用として設定すれば、各装置で、著作権保護用制御データを識別できる。後述する認証・鍵交換要求および認証・鍵交換手順で利用することが可能である。

【0040】さて、以下では、本実施形態の動作について説明する。なお、著作権保護の仕組みとしては、例えばDTCP（Digital Transmission Content Protection）の仕組みを用いた場合を想定して説明する（なお、他の著作権保護の仕組みを用いても構わない）。DTCPについては、

<http://www.dtcp.com>に詳しい。

【0041】図6に、本家庭ネットワークにおけるシーケンス例を示す。なお、図7に、無線AV送信装置1の認証・鍵交換に関する手順の一例を示し、図8に、無線AV受信装置2の認証・鍵交換に関する手順の一例を示す（なお、以下の各シーケンス例についても、無線AV送信装置1及び有線AV受信装置3の認証・鍵交換に関する手順の一例は、図7及び図8と同様である）。

【0042】ここでは、無線AV受信装置2が、無線AV送信装置1に対して、AVデータの送信を要求する場合を例にとって考える。このとき、例えばAV/Cプロトコル（1394トレードアソシエーションが規定した、AV機器制御用のコマンド、及びそのプロトコル）や、RTSP（IETFが規定した、WebサーバのAVストリーミング機能の遠隔制御用のプロトコル）を使って、TCP/IP上にコマンド（プロトコル）のやり取りを行なう（S1）。

【0043】すると、無線AV送信装置1は、上記コマンドを受け付け、無線AV受信装置2に対して、AVデータの送信を開始する（S2，S3，S121）。このAVデータの送信は、TCP/IPのバケット（あるいはUDP/IPのバケットでも良い）にて行なわれる。実際には、図9に示すように、転送されるAVデータは、RTP（リアルタイムトランスポートプロトコル）

（IETFにて標準化された、AVデータ転送用の転送プロトコル）にて転送されても良い。ここで、送信するデータは、著作権保護により保護すべきAVデータであるとする。この場合、RTPにて転送されるAVデータは、暗号化がなされた上で転送される（S2）。また、RTPバケットには、CCI（コピー制御情報）や、暗号管理情報、暗号再計算タイミング等の著作権保護用制御データが付与された形で、（暗号化された）AVデータが転送される。

【0044】これを受信した無線AV受信装置2は、受信したAVデータに暗号がかけられていることを発見しあるいはAVデータが暗号化されて転送されてくることを事前に察知するなりして（S101）、無線AV送信装置1に対して、暗号鍵（ここでは、暗号鍵＝復号鍵とする）の入手を試みるべく認証・鍵交換手順を要求し

（S4，S102，S122）、これを契機として、無線AV送信装置1と無線AV受信装置2との間で、認証・鍵交換手順を行う（S5；S103，S123）。

【0045】この際の認証・鍵交換の要求（S4）及び実際の認証・鍵交換手順（S5）は、図5にあるようなTCP/IPバケット上で行なわれるのではなく、図10にあるように、無線レイヤフレームに、AKE（認証・鍵交換）用のデータが直接搭載される形にて行なわれる。この無線レイヤヘッダのうち、「その無線レイヤフレームが、どのようなプロトコルのためのフレームであるか」を表示するフィールドとして、著作権保護プロト

コルであること（例えば、DTCIPであること）を意味する数値が入ることにもして良い。このようにすることにより、著作権保護（AKE）用のフレームが転送されていることが、受信側のノードは認識することができるようになる。

【0046】また、このAKE手順は、無線レイヤフレームを用いて行なわれるため、このAKE手順が無線ネットワーク5内に留まって処理されることが確実に保証される。

【0047】つまり、かりにTCP/IPバケットにてAKE手順を行なう場合を考えると、その場合には、隣の家同士や長距離あるいは国境を越えて（TCP/IPバケットが届くので）AKEバケットを交換することができるようになり、例えば著作権法30条の私的使用の範囲を越える範囲でのAVデータの転送（コピーを含む）がなされてしまう場合があり得る。

【0048】これに対して、本実施形態のようにAKE手順を無線レイヤフレームを用いて行なうことで、AKEがなされる最大範囲は、同一の無線ネットワーク上の中に留まることが保証される。なぜなら、無線レイヤフレームは、無線ネットワークを越えて転送されることが出来ないからである。

【0049】もちろん、この仕組みを強固にするために、「AKE手順を転送している無線フレームは、必ず、対向側のネットワークにブリッジ接続しない」という無線基地局やブリッジ装置を作成すると、上記の保証をより完全に行なうことが出来る。

【0050】さて、上記の認証・鍵交換手順が終了すると、無線AV送信装置1と無線AV受信装置2との間で、暗号鍵の値の共有が行なえる状態になっていることを意味する。繰り返すと、この状態（2つのノード間で暗号鍵の値が共有できる状態）は、同じ無線ネットワーク5に接続されたノード同士に限定される。つまり、無線AV送信装置1と無線AV受信装置2の間では、無線レイヤ制御バケットの転送が可能なので、上記AKE手順が成立することが可能である。一方、無線AV送信装置1と有線AV受信装置3の間では、AKEのためのバケット（フレーム）のやりとりが、無線AV送信装置1から見て、無線基地局4から向こう側（無線基地局から、有線AV受信装置間）では不可能であるため、AKE手順が成功することがない。このことから、著作権保護が通用する区間を「無線ネットワーク内（それも、1つのIPサブネット内）」という形に限定することが可能となる。

【0051】このようにして、「無線ネットワークをこえたAKE、ひいては不当なAVデータの転送」を未然に防ぐことが可能となる。

【0052】さて、上記では、無線レイヤフレーム上で直接AKE用のデータのやり取りを行なうことで、著作権保護の仕組み（正式なAVデータ受信装置が、受信し

た暗号化AVデータの復号化ができる仕組み)が有効である範囲を、無線ネットワーク内に限定することが可能であった。

【0053】これに代えて、著作権保護の仕組みが有効である範囲を、「イーサネットフレームが届く範囲」と限定することも可能である。

【0054】これは、図11のように、AKE制御データの転送を、イーサネットフレーム上にて直接行なうことによって、実現可能である。つまり、イーサネットフレームが、イーサネットパケットが届く範囲内の、IPサブネット内と限定することが可能であるため、(TCP/IPパケットを用いる代わりに)このイーサネットフレームを用いてAKE手順を行なえば、このAKEが成立する範囲を、イーサネットフレームが届く範囲(通常、ブリッジ接続を許容した1つのIPサブネット内)と限定することが可能となる。

【0055】図12に、このような場合のシーケンス例を示す。

【0056】図12のように(なお、前述したように、この場合の無線AV送信装置1及び有線AV受信装置3の認証・鍵交換に関する手順の一例は、図7及び図8と同様である)、無線ネットワーク5上の無線AV送信装置1と、イーサネット6に接続された有線AV受信装置3との間でのAKEのやり取りも可能となる。この場合は、IPルータを越えてAKEのやり取りが転送されることを未然に防ぐことが可能であるため、著作権保護されたAVデータの届く範囲(暗号が復号化されてしまう範囲)を、イーサネットフレームが転送される同一サブネット内に限定することが可能になる。

【0057】もちろん、この仕組みを強固にするために、「AKE手順を転送しているイーサネットフレームは、必ず、異なるサブネットワークにルーティングしない」というルータ装置を作成すると、上記の保証をより完全に行なうことが出来る。

【0058】なお、例えば、図1の例においては、無線AV送信装置1は、認証・鍵交換手順に無線レイヤフレームのみを用いる構成を採用することも、イーサネットフレームのみを用いる構成を採用することも、無線レイヤフレームとイーサネットフレームを適宜選択して使用する構成を採用することも可能である。

【0059】また、図6や図12の手順において、AVデータ転送が開始された後に認証・鍵交換要求及び認証・鍵交換手順を行ったが、AVデータ転送が開始される以前に認証・鍵交換要求及び認証・鍵交換手順を行う構成も可能である。また、図6や図12の手順において、AVデータの転送が完了してから、認証・鍵交換要求及び認証・鍵交換手順を行うようにしてもよいし、AVデータの転送の途中で、認証・鍵交換要求及び認証・鍵交換手順を行うようにしてもよい。また、図6や図12の手順において、認証・鍵交換要求及び認証・鍵交換手順

に成功した後に、あらためて暗号化されたAVデータを最初から転送する構成も可能である。また、図6や図12の手順において、認証・鍵交換要求や認証・鍵交換手順において、一方の装置から他方の装置にあるメッセージを出し、該他方の装置から該一方の装置に該あるメッセージに対する応答を返す際に、該一方の装置が該あるメッセージを出してからこれに対する該応答を受けるまでの時間が、予め定められた基準時間を超える場合には、該認証・鍵交換要求や認証・鍵交換手順を中止するようにしてもよい。これらの点は、以下の各シーケンス例についても同様である。

【0060】さて、以下では、無線レイヤフレームもしくはイーサネットフレーム上にて送信装置と受信装置との間でやり取りされる認証・鍵交換(AKE)手順のバリエーションを説明する。

【0061】なお、以下では、無線レイヤフレームもしくはイーサネットフレームのいずれかを用いるものとする。図1の例の場合、無線AV受信装置2に対しては、無線レイヤフレームとイーサネットフレームの両方が使用でき、有線AV受信装置3に対しては、イーサネットフレームが使用できる。

【0062】また、ここでは、無線AV受信装置2と有線AV受信装置3を総称して、AV受信装置と呼ぶものとする。

【0063】AKEは、特定のRTPストリームによって転送されるAVストリームに関して行なわれるものである。このため、AKEを行なう前提として、「どのAVストリームに関するAKEなのか」についての交渉を行なう必要がある場合がある。例えば、AV受信装置が、受信したAVストリームが暗号化されていることを認識し、「このAVストリームについてのAKEをさせて欲しい」と無線AV送信装置に問い合わせる場合がある。また、無線AV送信装置が、「このAVストリームは、暗号化してAV受信装置に対して送出する。このことを、予め、あるいは、AVストリーム転送と同時に、AV受信装置に対して通知し、AKEのトリガをかけさせる必要がある」と判断し、AV受信装置に対して、「このAVストリームは暗号化して送信する。よって、このAVストリームについてAKE手順を自装置(無線AV送信装置)に対して行なうべし」という通知を行なう場合が考えられる。

【0064】もちろん、1本1本のAVストリーム毎にAKEを行なうのではなく、「無線AV送信装置と、AV受信装置との間でやり取りされる、全てのRTPストリームに関して有効とするためのAKE」を一度に行なってしまう、その後は、無線AV送信装置とAV受信装置との間でやり取りされる全てのRTPストリームに関しても、このAKE手順により定められた条件に従って、AVデータの暗号化が行なわれるようになっていても良い。

【0065】その場合、どのポート番号の通信においては、どのような著作権保護制御情報（暗号管理情報や暗号再計算タイミング等）を用いるものであるかについての情報交換を行ってもよい。

【0066】図13に、AV受信装置（2あるいは3）側が、無線AV送信装置1に対してAKEのトリガを最初にかける場合についてのシーケンスの例を示す。

【0067】なお、無線AV送信装置のIPアドレスをa、送信ポート番号を#xとし、AV受信装置のIPアドレスをb、受信ポート番号を#yとする。

【0068】これまでの手順と同様に、AV受信装置から無線AV送信装置へ、AV制御コマンドが出され、無線AV送信装置は、AVデータを暗号化して、AV受信装置へ転送する（S21、S22、S23）。

【0069】ここで、AV受信装置は、何らかの方法で、受信したAVストリームが暗号化されていることを認識する。例えば、「受信したAVストリームを復号しても、所望のAVストリームが再生できない場合」、あるいは「受信したAVストリームに、図9に示したような著作権保護用の制御データが付属しており、これを検出して、そのAVストリームが暗号化されていることを認識する場合」等が考えられる。

【0070】受信したAVストリームが暗号化されていること、あるいはその可能性があることを認識したAV受信装置は、認証・鍵交換要求を無線AV送信装置に対して送出する（S24）。なお、前述したように、これを、無線レイヤパケットを使って行なう場合と、イーサネットフレームを使ってこれを行なう場合が可能である。なお、そのプロトコルフィールドの値として、例えば「DTCP」を意味する値を持つようにしても良い。すなわち、この手順もDTCPの手順の一部とすることが可能である。

【0071】その際、AV受信装置は、そのAKE要求（あるいは、後続のAKE手順パケット）にて、「どのAVストリームについてのAKEであるか」を明示する。例えば、無線AV送信装置のIPアドレスとポート番号及びAV受信装置のIPアドレスとポート番号を、そのAKE要求に明記する（S24参照）。また、対象とするAVストリームを特定する他の方法として、RTPのSSRCフィールドの値（AVソース毎に一覧につけられる識別番号であり、例えば、RTPのスペックであるRFC1889に詳しい）を用いて、この番号をAKE要求に明記しても良い。また、IPv6パケット等に含まれる「フローID」の値を用いても良い。その他の方法も可能である。

【0072】また、この要求に、暗号管理情報や暗号再計算タイミング等についての情報が含まれていてもよい。

【0073】また、無線AV送信装置と、AV受信装置との間には、複数のAVストリーム（例えば、映像と音

声）が同時にやり取りされている場合があるので、この「どのAVストリームについてのAKEであるか」についての情報（例えば、送信装置と受信装置のIPアドレスとポート番号の組の情報、又はSSRCの値やフローIDの値、又はこれらの組み合わせ）に、一度に複数のAVストリームを指定できるようになっていても良い。

【0074】このようなAKE要求を受信した無線AV送信装置は、そのAKE要求（あるいは、AKE手続き）が、どのAVストリームのためのものであるかを認識した上で、AKE手順を継続する（S25）。

【0075】結局、AKE手順が終了すると、AV受信装置は、そのAKE結果をもとに、その暗号化AVストリームの復号鍵を取得（あるいは、復号鍵を取得するための計算のための初期情報を取得）することが可能になる（S26）。

【0076】次に、図14に、無線AV送信装置1側が、AV受信装置（2あるいは3）に対して、あるAVストリームについて、「このAVストリームは暗号化して送信する」旨を通知し、これをトリガとして、AV受信装置が無線AV送信装置に対してAKE要求をかける場合についてのシーケンスの例を示す。

【0077】S31～S33については、図13のシーケンス例のS21～S23と同様である。

【0078】このシーケンス例では、無線AV送信装置は、AV受信装置に対して送信するAVストリームが、DTCP等のプロトコルに従って暗号化され、これをAV受信装置が復号するには、無線AV送信装置との間でAKEを行なう必要があることをAV受信装置に対して通知する（S34）。この通知は、IPパケットを用いて行なっても良いが、このシーケンス例では、その後で行われるAKE手順と同様に、無線レイヤパケットもしくはイーサネットフレームを用いて行なわれるものとする。

【0079】S34～S36は、図13のシーケンス例のS23～S25と同様である。

【0080】すなわち、受信するAVストリームあるいは受信したAVストリームが暗号化されることを認識したAV受信装置は、認証・鍵交換要求を送信装置に対して送出する（S35）。AKE要求を受信した無線AV送信装置は、そのAKE要求（あるいは、AKE手続き）が、どのAVストリームのためのものであるかを認識した上で、AKE手順を継続する（S36）。AKE手順が終了すると、AV受信装置は、そのAKE結果をもとに、その暗号化AVストリームの復号鍵を取得（あるいは、復号鍵を取得するための計算のための初期情報を取得）することが可能になる（S37）。

【0081】さて、これまでの説明では、従来のDTCPと同様に、転送されるAVストリームには、図9と同様に、著作権保護用の制御データが付与されることを想定していた。この著作権保護用の制御データは、例え

ば、そのAVストリームの暗号管理情報（例えば、そのAVストリームが、コピー自由（copy free）であるか、1回コピー可能（copy once）であるか、更なるコピーは不可であるか（no more copy）、コピー不可（never copy）であるかについての情報）や、暗号鍵の再計算タイミング（例えば、どのRTPシーケンス番号のときに特定の暗号鍵を使用しはじめ、続いて同シーケンス番号のいくつおきに、暗号鍵を再計算すべきか、についての情報）を通知するためのフラグ等が含まれる。ところが、場合によっては、転送されるAVストリームに、著作権保護用の制御データを付与できない場合（つまり、RTPパケットをそのまま転送する必要がある場合）が考えられる。

【0082】図15、このような場合のAVストリームの転送フォーマットの例を示す。

【0083】図15の例は、基本的には、図9から、著作権保護用制御データを取り去ったもの、すなわち通常のRTPパケット（ただし、そのペイロードのAVストリームが暗号化されたもの）のフォーマットとなる。

【0084】このような場合には、事前に（あるいは、該AVストリーム転送中に）、「そのAVストリームの暗号管理情報」や、「何パケット毎に、AVストリームの暗号鍵を再計算すべきか」についての情報を、前述のAKE手順で行なえばよい。

【0085】図16に、この場合のシーケンス例を示す。

【0086】例えば、無線AV送信装置が、転送するAVストリームについての暗号管理情報や、AVストリーム暗号鍵の再計算タイミングを、AKE手順中にて、AV受信装置に対して通知する（S43参照）。

【0087】このようにすることにより、転送されるAVストリームに著作権保護用の制御データを付与しなくても、送信側と受信側で、暗号管理情報や、暗号鍵の再計算のタイミングを予め共有することが可能となり、ひいては、送信側から受信側に対して、セキュアなAVストリームの転送を実現することが可能になる。

【0088】図16では、AV受信装置からトリガがかかる例であるが、もちろん無線AV送信装置からAV受信装置に対して最初に通知する場合においても、同様に行なうことが可能である（例えば、図14のシーケンス例のS36において行うことが可能である）。

【0089】なお、図1では、無線AV送信装置が存在したが、その代わりにまたはそれに加えて、同様の機能をする有線AV送信装置が存在してもよい（有線AV送信装置の構成例は、図2のインタフェースを修正したものである；この修正は、図3の無線AV受信装置から図4の有線AV受信装置への修正と同様である）。ただし、有線AV送信装置は、無線レイヤフレームを使用できないので、イーサネットフレーム上で認証・鍵交換を

行う機能を有することになる。したがって、図1においては、有線AV送信装置は、無線AV受信装置と有線AV受信装置のいずれとも認証・鍵交換を行うことができることになる。

【0090】また、図1では、イーサネット（有線ネットワーク）と無線ネットワークが存在したが、無線ネットワークのみ存在してもよい。この場合、無線AV送信装置と無線AV受信装置との間で、無線レイヤフレーム上で認証・鍵交換を行うことができる（なお、イーサネットフレーム上で認証・鍵交換を行ってもよい）。あるいは、逆に、イーサネット（有線ネットワーク）のみ存在してもよい。この場合、有線AV送信装置と有線AV受信装置との間で、イーサネットフレーム上で認証・鍵交換を行うことができる。

【0091】また、例えば、図1のイーサネットに、更に他の異なる（1又は複数の）無線基地局及び無線ネットワークが接続されていてもよい。あるいは、図1の無線ネットワークに、更に他の異なる（1又は複数の）イーサネットが接続されていてもよい。家庭ネットワークの構成がどのようなになっていても、無線レイヤフレームあるいはイーサネットフレームの到達する範囲内でのみ、認証・鍵交換を行うことができる。

【0092】なお、以上で想定したプロトコルは、一例であり、同様の性質を持つ他のプロトコルについても本発明は適用可能である。

【0093】また、以上では、ローカルエリアネットワークとして家庭ネットワークを例にとり説明したが、もちろん、企業内網など他のローカルネットワークであっても本発明は同様に適用可能である。

【0094】また、以上では、AVコンテンツの暗号処理について、暗号鍵＝復号鍵を想定して説明したが、暗号鍵≠復号鍵となる場合にも、本発明は適用可能である。

【0095】なお、以上の各機能は、ソフトウェアとして実現可能である。また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータに所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムとして実施することもでき、該プログラムを記録したコンピュータ読取り可能な記録媒体として実施することもできる。

【0096】なお、この発明の実施の形態で例示した構成は一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能あるいは要素を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能

である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。また、この発明の実施の形態で例示した各種構成部分についての各種バリエーションは、適宜組み合わせる実施することが可能である。また、この発明の実施の形態は、個別装置としての発明、関連を持つ2以上の装置についての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またはカテゴリに係る発明を包含・内在するものである。従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【0097】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0098】

【発明の効果】本発明によれば、著作権を保護すべきコンテンツ・データを暗号化して転送し復号して利用できる範囲を、一定の範囲内に制限することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るネットワークシステムの構成例を示す図

【図2】同実施形態に係る無線AV送信装置の構成例を示す図

【図3】同実施形態に係る無線AV受信装置の構成例を示す図

【図4】同実施形態に係る有線AV受信装置の構成例を示す図

【図5】同実施形態に係る無線レイヤフレームのフォーマットの一例を示す図

【図6】同実施形態に係るネットワークシステムの全体のシーケンスの一例を示す図

【図7】同実施形態に係る無線AV送信装置の認証・鍵交換に関する手順の一例を示すフローチャート

【図8】同実施形態に係る無線AV受信装置及び有線A

V受信装置の認証・鍵交換に関する手順の一例を示すフローチャート

【図9】同実施形態に係るIPパケットによるAVデータ転送フォーマットの一例を示す図

【図10】同実施形態に係る認証・鍵交換用データの転送方法の一例について説明するための図

【図11】同実施形態に係る認証・鍵交換用データの転送方法の他の例について説明するための図

【図12】同実施形態に係るネットワークシステムの全体のシーケンスの他の例を示す図

【図13】同実施形態に係るネットワークシステムの全体のシーケンスのさらに他の例を示す図

【図14】同実施形態に係るネットワークシステムの全体のシーケンスのさらに他の例を示す図

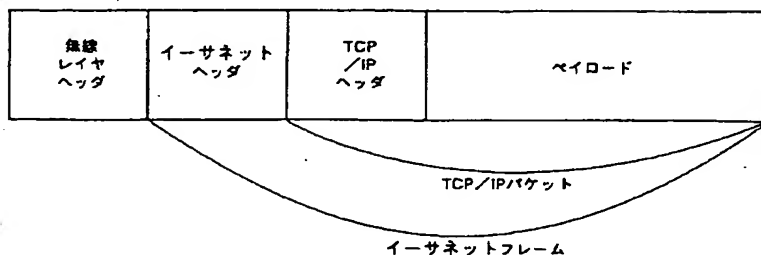
【図15】同実施形態に係るIPパケットによるAVデータ転送フォーマットの他の例を示す図

【図16】同実施形態に係るネットワークシステムの全体のシーケンスのさらに他の例を示す図

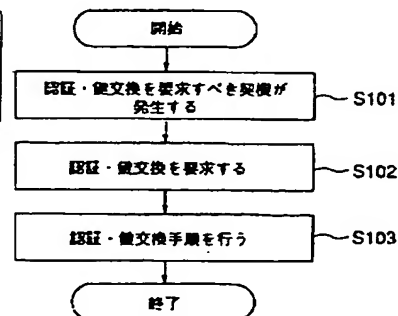
【符号の説明】

- 1…無線AV送信装置
- 2…無線AV受信装置
- 3…有線AV受信装置
- 4…無線基地局
- 5…無線ネットワーク
- 6…イーサネット
- 11…AVデータ生成/蓄積部
- 12, 22, 32…RTP処理部
- 13, 23, 33…TCP/IPパケット送受信部
- 14, 24, 34…著作権保護暗号化部
- 15, 25, 35…イーサネットフレーム送受信部
- 16, 26, 36…IP/イーサネットアドレス対応テーブル
- 17, 27, 37…著作権保護認証・鍵交換部
- 18, 28…無線ネットワークI/F部
- 21, 31…AVデータ再生/蓄積部
- 38…イーサネットI/F部

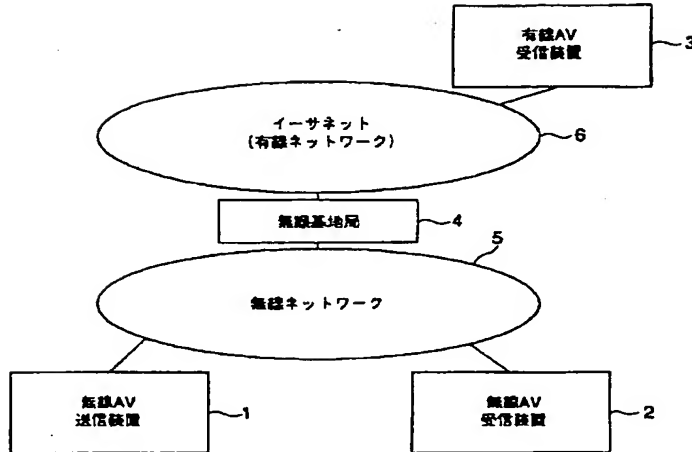
【図5】



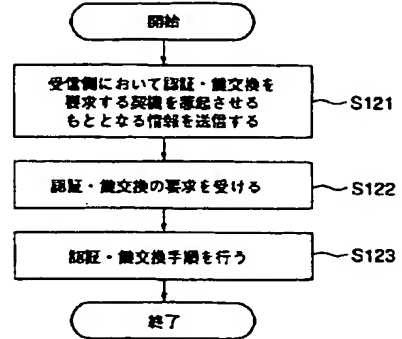
【図7】



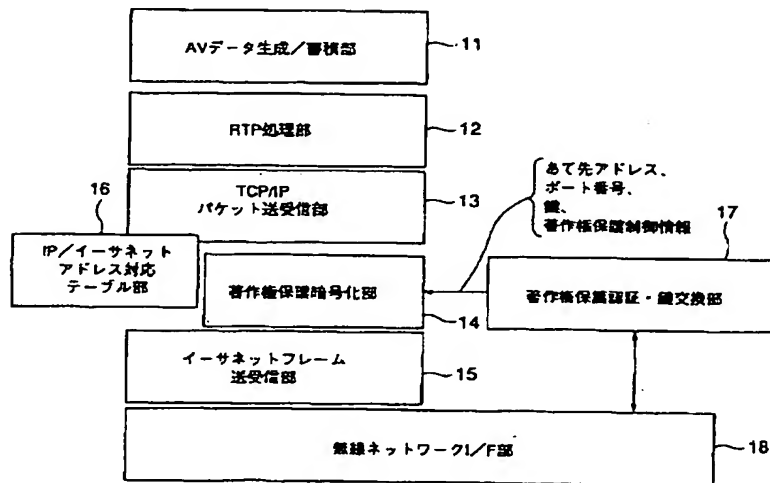
【図1】



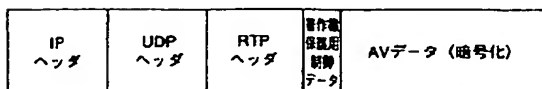
【図8】



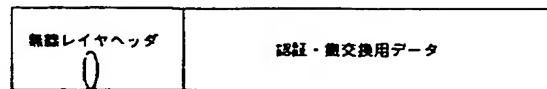
【図2】



【図9】

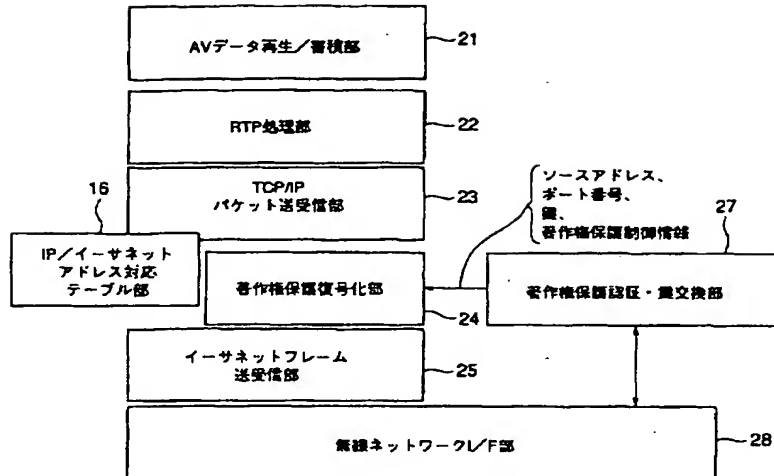


【図10】

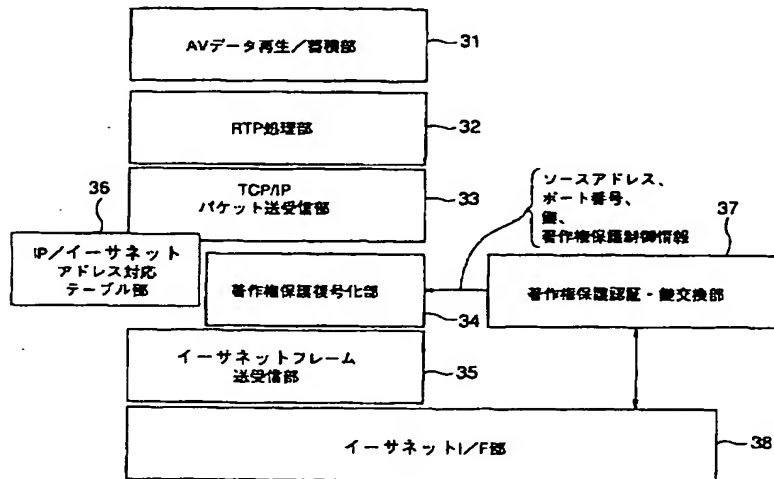


プロトコルタイプ-著作権保護プロトコル(例: DTCP)

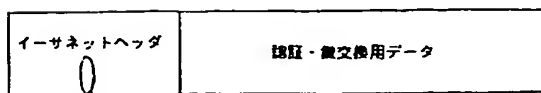
【図3】



【図4】

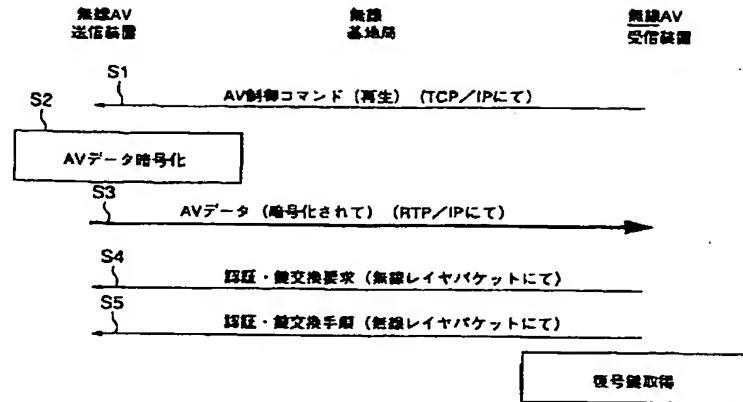


【図11】

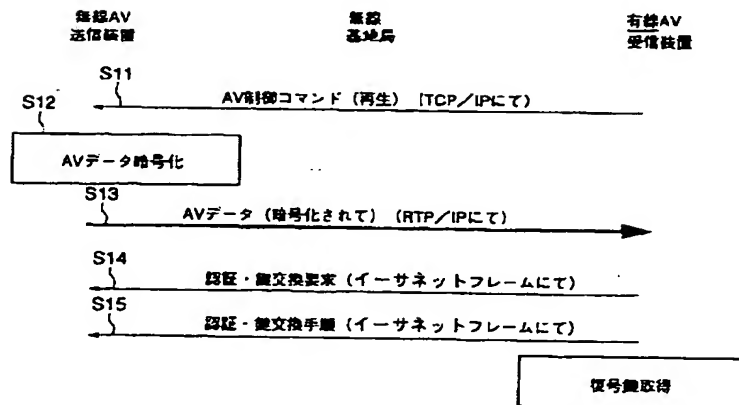


プロトコルタイプ=著作権保護プロトコル (例: DTCP)

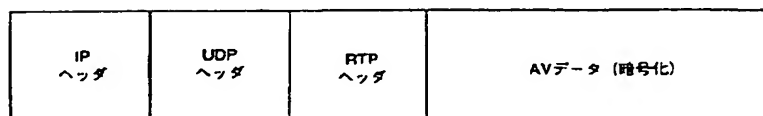
【図6】



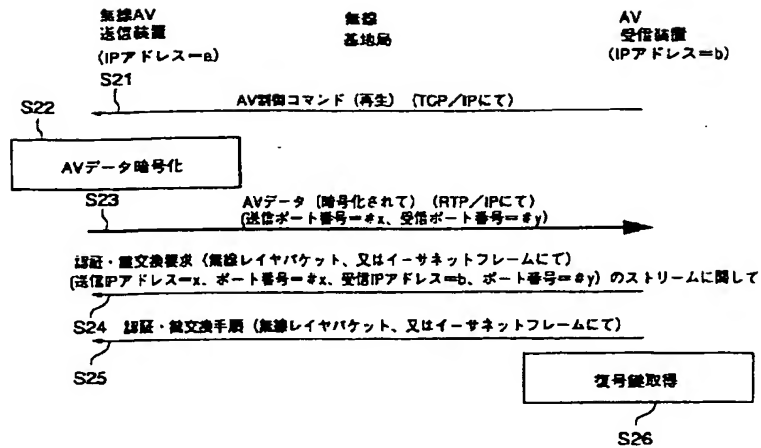
【図12】



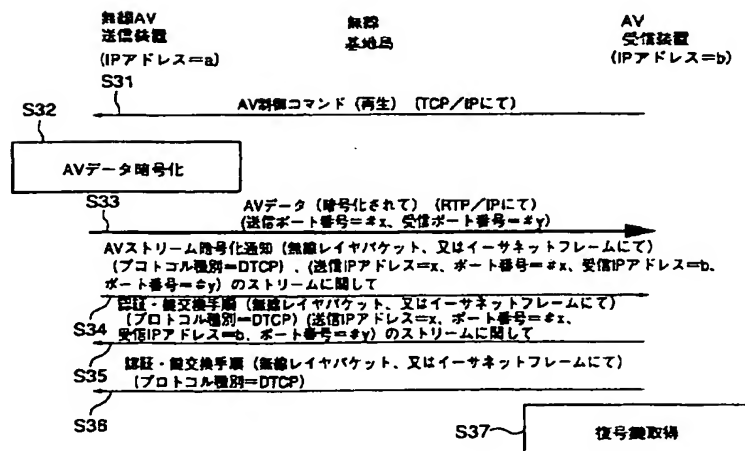
【図15】



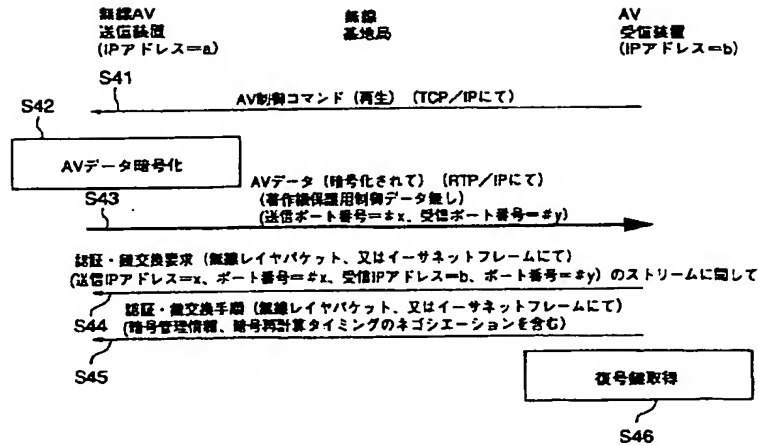
【図13】



【図14】



【図16】



フロントページの続き

(72)発明者 角田 啓治
神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

Fターム(参考) SJ104 AA07 EA02 EA15 KA01 KA04
NA02
SK033 AA08 BA01 CB11